

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

METHOD AND DEVICE FOR PROTECTING COPYRIGHT

Patent Number: JP9320192
Publication date: 1997-12-12
Inventor(s): SAKAI YASUYUKI; CHIKASAWA TAKESHI; YAMAGISHI ATSUHIRO; TAKEDA EISAKU; OGAWA MASAHARU
Applicant(s): MITSUBISHI ELECTRIC CORP
Requested Patent: ☐ JP9320192
Application Number: JP19960133523 19960528
Priority Number (s):
IPC Classification: G11B20/10; G06F3/06; G06F12/14; G09C1/00; H04L9/08
EC Classification:
Equivalents:

Abstract

PROBLEM TO BE SOLVED: To prevent the data from being improperly copied by adding to the digital data copy control information, discriminative information, etc., of ciphering algorithm.
SOLUTION: The digital data error corrected by an error correction circuit 205 are inputted to a data format means 206, and a header for protecting copyright is added to the top of the data. The header is constituted of ciphering start information, a ciphering key, a unit of ciphering, the copy control information showing the information on whether or not the copy of the data is allowed and the discriminative information of the used ciphering algorithm. The ciphering key is a random number information generated by a key delivery means 210, and the header itself contains also another random number information, shared with procedure by a Diffy-Helman type key delivery system as key information. The improper copy of the data is prevented since the data added with the header are ciphering processed when the copy is not allowed.

Data supplied from the esp@cenet database - 12

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-320192

(43) 公開日 平成9年(1997)12月12日

(51) Int.Cl. ⁹	識別記号	庁内整理番号	F I	技術表示箇所
G 1 1 B 20/10		7736-5D	G 1 1 B 20/10	H
G 0 6 F 3/06	3 0 4		G 0 6 F 3/06	3 0 4 M
	12/14			3 1 0 K
G 0 9 C 1/00	6 3 0	7259-5 J	G 0 9 C 1/00	6 3 0 A
H 0 4 L 9/08			H 0 4 L 9/00	6 0 1 A
審査請求 未請求 請求項の数3 O L (全 6 頁)				

(21) 出願番号 特願平8-133523

(22) 出願日 平成8年(1996)5月28日

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 酒井 康行

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(72) 発明者 近澤 武

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(72) 発明者 山岸 篤弘

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(74) 代理人 弁理士 宮田 金雄 (外3名)

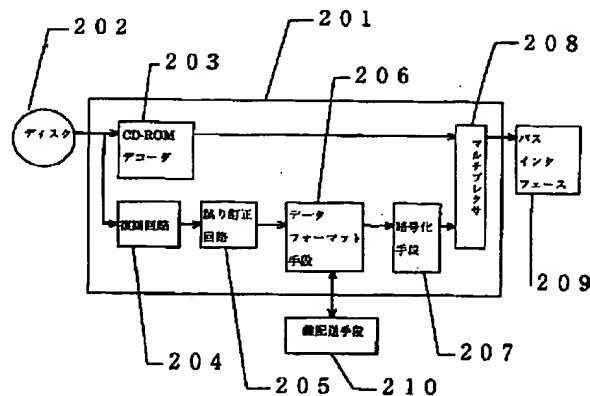
最終頁に続く

(54) 【発明の名称】 著作権保護方法及び装置

(57) 【要約】

【課題】 著作権者の権利を保護できる著作権保護方法及び装置を得ることを課題とする。

【解決手段】 ディスクから読み出されたデジタル情報に、暗号化開始情報、暗号化鍵、暗号化の単位、データの複製を許可するか否かの情報を示す複製管理情報、及び使用する暗号化アルゴリズムの識別情報を付加するデータフォーマット手段206と、前記デジタル情報を暗号化する暗号化手段とを備えた。



【特許請求の範囲】

【請求項1】 デジタル情報に、暗号化開始情報、暗号化鍵、暗号化の単位、データの複製を許可するか否かの情報を示す複製管理情報、及び、使用する暗号化アルゴリズムの識別情報を付加することを特徴とする著作権保護方法。

【請求項2】 デジタル情報に、暗号化開始情報、暗号化鍵、暗号化の単位、データの複製を許可するか否かの情報を示す複製管理情報、及び、使用する暗号化アルゴリズムの識別情報を付加するデータフォーマット手段と、前記デジタル情報を暗号化する暗号化手段とを備えたことを特徴とする著作権保護装置。

【請求項3】 暗号化デジタル情報に付加された、暗号化開始情報、暗号化鍵、暗号化の単位、データの複製を許可するか否かの情報を示す複製管理情報、及び、使用する暗号化アルゴリズムの識別情報を復号するデータフォーマット手段と、このデータフォーマット手段により復号された情報に基づいて前記暗号化デジタル情報を復号する復号手段とを備えたことを特徴とする著作権保護装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、データの不正な複製を防ぐことができる著作権保護方法及び装置に関する。

【0002】

【従来の技術】従来のDVD (Digital Video Disc) を再生する装置およびそこで使用されているデータフォーマットについて説明する。

【0003】図6は、DVDを再生する装置で用いられている従来のデータフォーマットを説明する図である。図において、601はデータフォーマット、602はヘッダー、603はデータ、604はテラーである。ヘッダー602には、著作権保護に関する情報が書き込まれている。

【0004】図7は、DVDを再生するための従来の光ディスクシステムである。図において701はDVDドライブ、702はDVD又はCD-ROMのディスク、703はCD-ROMデコーダ、704は復調回路、705は誤り訂正回路、706はマルチプレクサ、707はバスインタフェースである。DVDドライブ701はDVDとCD-ROMの両方のディスクを再生できるように構成されている。次に動作を説明する。ディスク702から読み出されたデータは、CD-ROMデコーダ703および復調回路704に入力される。CD-ROMデコーダ703ではCD-ROMの場合の復調、誤り訂正が行われる。復調回路704ではディスク702から読み出された信号をデジタルデータに復調する。復調されたデータは、誤り訂正回路705に入力され、DVDフォーマットのデータの誤り訂正を行う。マルチプ

レクサ706では、ディスク702がDVD、CD-ROMのいずれであるかに応じてデータを選択し、バスインタフェース707に出力する。

【0005】

【発明が解決しようとする課題】従来の光ディスクシステムは、ディスクに記録されているデジタルデータを何ら加工せず、記録されているままに再生していた。そのため、ディスクに記録されているデータの複製を作ることが容易であり、データの著作権者の権利を保護することが困難であるという課題があった。

【0006】本発明の目的は、係る課題を解決するためになされたもので、データの複製を作ることが困難で、著作権者の権利を保護することができる著作権保護方法及び装置を得ることにある。

【0007】

【課題を解決するための手段】本発明の請求項1に係る著作権保護方法は、デジタル情報に、暗号化開始情報と、暗号化鍵と、暗号化の単位と、データの複製を許可するか否かの情報を示す複製管理情報と、使用する暗号化アルゴリズムの識別情報とを付加するものである。

【0008】本発明の請求項2に係る著作権保護装置は、デジタル情報に、暗号化開始情報、暗号化鍵、暗号化の単位、データの複製を許可するか否かの情報を示す複製管理情報、及び、使用する暗号化アルゴリズムの識別情報を付加するデータフォーマット手段と、前記デジタル情報を暗号化する暗号化手段とを備えたものである。

【0009】本発明の請求項3に係る著作権保護装置は、暗号化デジタル情報に付加された、暗号化開始情報、暗号化鍵、暗号化の単位、データの複製を許可するか否かの情報を示す複製管理情報、及び、使用する暗号化アルゴリズムの識別情報を復号するデータフォーマット手段と、このデータフォーマット手段により復号された情報に基づいて前記暗号化デジタル情報を復号する復号手段とを備えたものである。

【0010】

【発明の実施の形態】

実施の形態1. 本発明による著作権保護方法の一実施の形態を図1に基づいて説明する。図1は、本実施の形態によるデータフォーマットを説明する図である。図において、101はデータフォーマット、102はヘッダー、103はデータ、104はテラーである。

【0011】次に動作を説明する。データ103はディスクに記録されていたデータであり、データ103の先頭に著作権保護のためのヘッダー102を付加する。ヘッダー102は次の情報から構成される。第1は暗号化スタート情報で、この情報以降のデータが暗号化されていることを示す。第2は暗号化鍵である。第3は暗号化の単位で、暗号化する情報の単位のバイト数を示す。第4は複製管理情報で、データの複製を許可するか否かの

情報を示す。データの複製を許可しないならば、データを暗号化することにより秘匿することができる。第5は暗号化アルゴリズムを示し、暗号化処理に用いる暗号アルゴリズムを、複数の中から選択できる。テラー104はデータの終了を示す。このヘッダー102を付加することにより、データの著作権者が複製を許可しない場合は、データを暗号化することができ、データの不正な複製を防ぐことができる。

【0012】実施の形態2. 本発明による著作権保護装置の一実施の形態を、図2に基づいて説明する。図2は、本実施の形態による著作権保護装置の構成図である。図において、201はDVDドライブ、202はDVD、又はCD-ROMのディスク、203はCD-ROMデコーダ、204は復調回路、205は誤り訂正回路、206はデータフォーマット手段、207は暗号化手段、208はマルチプレクサ、209はバスインタフェース、210は鍵配送手段である。

【0013】次に動作を説明する。DVDドライブ201は、DVD、CD-ROMいずれのディスクも再生できるように構成されている。ディスク202から読み出されたデータは、CD-ROMデコーダ203および復調回路204に入力される。CD-ROMデコーダ203ではCD-ROMの場合の復調、誤り訂正が行われる。復調回路204ではディスク202から読み出された信号をデジタルデータに復調する。復調されたデータは、誤り訂正回路205に入力され、DVDフォーマットのデータの誤り訂正を行う。誤り訂正されたデータは、データフォーマット手段206に入力され、前記ヘッダー102およびテラー104が付加される。次に暗号化手段207に入力され、ヘッダー102の情報に基づいて暗号化処理が行われる。マルチプレクサ208では、ディスク202がDVD、CD-ROMのいずれであるかに応じてデータを選択し、バスインタフェース209にデータを出力する。データフォーマット手段206において付加される暗号化鍵は、鍵配送手段210により生成される乱数情報であり、ヘッダー102自身もディフィーヘルマン型鍵配送方式による手順により共有化される別の乱数情報を鍵情報として暗号化される。ディフィーヘルマン型鍵配送方式は公知の技術であり、例えば、池野、小山著、電子情報通信学会編、「現代暗号理論」に記載されている。本実施の形態の著作権保護装置は、データフォーマット手段206と暗号化手段207と鍵配送手段210とを備えていることにより、バスインタフェース209に出力されるデータには、著作権者の意図により暗号化を施すことができるので、データの不正な複製を防ぎ、著作権者の権利を保護することができる。

【0014】実施の形態3. 本発明による著作権保護装置の一実施の形態を、図3に基づいて説明する。図3は、本実施の形態による著作権保護装置の構成図であ

る。図において、301はDVDドライブ、302はDVD又はCD-ROMのディスク、303はCD-ROMデコーダ、304は復調回路、305は誤り訂正回路、306はマルチプレクサ、307はデータフォーマット手段、308は暗号化手段、309はバスインタフェース、310は鍵配送手段である。

【0015】次に動作を説明する。DVDドライブ301は、DVD、CD-ROMいずれのドライブも再生できるように構成されている。ディスク302から読み出されたデータは、CD-ROMデコーダ303および復調回路304に入力される。CD-ROMデコーダ303ではCD-ROMの場合の復調、誤り訂正が行われる。復調回路304ではディスク302から読み出された信号をデジタルデータに復調する。復調されたデータは、誤り訂正回路305に入力され、DVDフォーマットのデータの誤り訂正を行う。マルチプレクサ306では、ディスク302がDVD、CD-ROMのいずれであるかに応じてデータを選択する。次に、データは、データフォーマット手段307に入力され、前記ヘッダー102およびテラー104が付加される。次に暗号化手段308に入力され、ヘッダー102の情報に基づいて暗号化処理が行われる。暗号化されたデータは、バスインタフェース309に出力される。データフォーマット手段307において付加される暗号化鍵は、鍵配送手段310により生成された乱数情報であり、ヘッダー102自身も、ディフィーヘルマン型鍵配送方式による手順で共有化される別の乱数情報を鍵情報として暗号化される。本実施の形態の著作権保護装置は、データフォーマット手段307と暗号化手段308と鍵配送手段310とを備えていることにより、バスインタフェース309に出力されるデータには、著作権者の意図により暗号化を施すことができるので、データの不正な複製を防ぎ、著作権者の権利を保護することができる。

【0016】実施の形態4. 本発明による著作権保護装置の一実施の形態を、図4に基づいて説明する。図4は、本実施の形態による著作権保護装置の構成図で、ディスクに記録されている映像等をディスプレイに表示する構成を示している。図において、401はバスインタフェース、402はコンピュータ、403はAVボード、404はデータフォーマット手段、405は復号手段、406はビデオ回路、407はディスプレイ、408は鍵配送手段である。

【0017】次に動作を説明する。バスインタフェース401には、前記発明の実施の形態2および3で説明した、ヘッダー付の暗号化されたデータが入力される。データはコンピュータ402を介してAVボード403に入力される。AVボード403内では、まずデータフォーマット手段404にデータは入力される。ここでは、ディフィーヘルマン型鍵配送方式により共有化された鍵情報により前記ヘッダー102を復号し、前記ヘッダー

102に含まれる情報に基づいて、暗号アルゴリズムの種類、暗号化の単位、暗号化鍵等の情報を、復号手段405に送信する。これに基づき復号手段405では、データの復号処理を行う。復号されたデータは、ビデオ回路406から、ディスプレイ407に表示される。データフォーマット手段404において出力される暗号化鍵は、鍵配送手段408により、ディフィーヘルマン型鍵配送方式による手順で共有化された別の鍵情報により暗号化することで暗号化されたヘッダー102に含まれる。本実施の形態の著作権保護装置は、データフォーマット手段404と復号手段405と鍵配送手段408とを備えていることにより、暗号化鍵を共有しない場合はデータを復号することができないので、データの不正にディスプレイ表示することを防ぐことができ、著作権者の権利を保護することができる。

【0018】実施の形態5. 本発明による著作権保護装置の一実施の形態を、図5に基づいて説明する。図5は、本実施の形態による著作権保護装置の構成図で、ディスクに記録されている映像等をディスプレイに表示する構成を示している。図において、501はバスインタフェース、502はコンピュータ、503はハードディスク、504はデータフォーマット手段、505は復号手段、506はAVボード、507はビデオ回路、508はディスプレイ、509は鍵配送手段である。

【0019】次に動作を説明する。バスインタフェース501には、前記発明の実施の形態2および3で説明した、ヘッダー付きの暗号化されたデータが入力される。データはコンピュータ502内に入力される。コンピュータ502内では次の動作をする。ハードディスク503内にデータを保存する場合、暗号化されているデータを復号するには、データフォーマット手段504、復号手段505を介さなければならない。つまり、鍵配送、例えば前記のディフィーヘルマン型鍵配送により正しい暗号化鍵を伝送されなければ、暗号を解くことはできない。したがって、不正な複製を防止することができる。データをディスプレイに表示する際にも、データフォーマット手段504、復号手段505により復号を行う。データフォーマット手段504において出力される暗号化鍵は、鍵配送手段509により、ディフィーヘルマン型鍵配送方式による手順で共有化された別の鍵情報により暗号化することで暗号化されたヘッダー102に含まれる。本実施の形態の著作権保護装置は、データフォー

マット手段504と復号手段505と鍵配送手段509とを備えていることにより、暗号化鍵を共有しない場合はデータを復号することができないので、データの不正にハードディスクに保存したり、ディスプレイに表示することを防ぐことができ、著作権者の権利を保護することができる。

【0020】実施の形態6. 前記実施の形態2、3、4および5では、暗号化鍵を共有するための秘密情報はあらかじめ装置内に保持していたが、秘密情報を外部から与えるように構成することも可能である。

【0021】実施の形態7. 前記実施の形態3では、データフォーマット手段は、DVDドライブ301より出力されたデジタル情報を入力して処理したが、DVDドライブ301でなくても良く、デジタル情報を出力する装置であれば良い。

【0022】

【発明の効果】以上のように本発明による著作権保護方法及び装置は、データの不正な再生、複製、およびディスプレイ表示を防ぐことができ、著作権者の権利を保護することができる効果がある。

【図面の簡単な説明】

【図1】 本発明の実施の形態1の著作権保護方法を説明する図である。

【図2】 本発明の実施の形態2の著作権保護装置の構成図である。

【図3】 本発明の実施の形態3の著作権保護装置の構成図である。

【図4】 本発明の実施の形態4の著作権保護装置の構成図である。

【図5】 本発明の実施の形態5の著作権保護装置の構成図である。

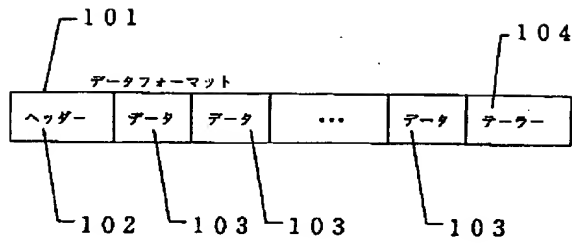
【図6】 従来のデータフォーマットを説明する図である。

【図7】 従来の光ディスクシステムの構成図である。

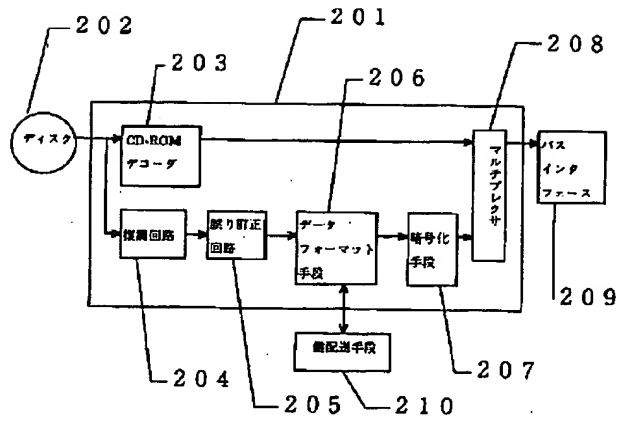
【符号の説明】

101 データフォーマット、102 ヘッダー、103 データ、104 テーラー、201 DVDドライブ、202 ディスク、203 CD-ROMデコーダ、204 復調回路、205 誤り訂正回路、206 データフォーマット手段、207 暗号化手段、208 マルチプレクサ、209 バスインタフェース、210 鍵配送手段。

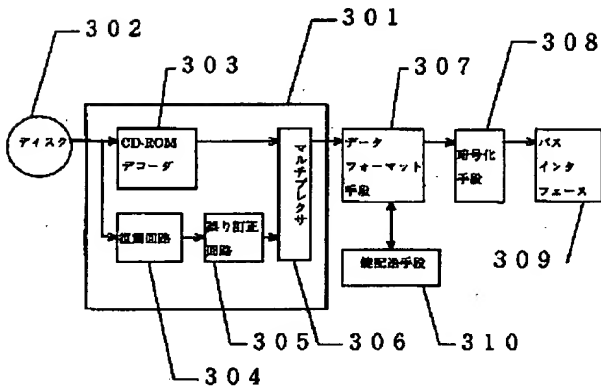
【図1】



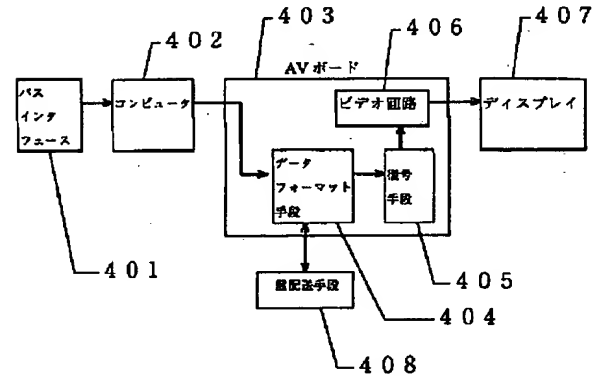
【図2】



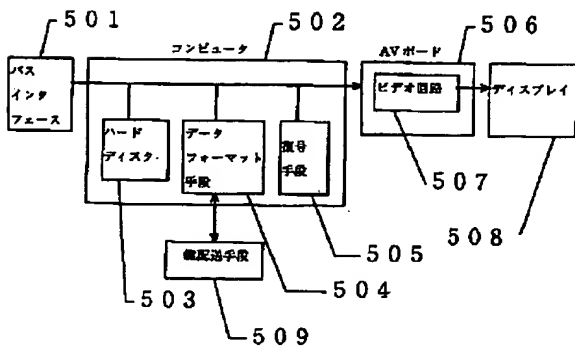
【図3】



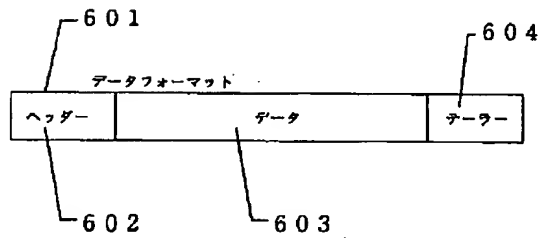
【図4】



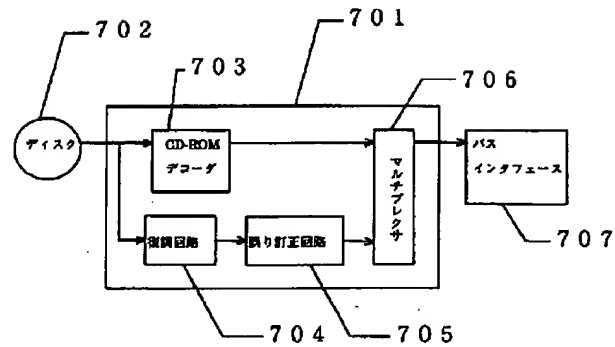
【図5】



【図6】



【図7】



フロントページの続き

(72)発明者 竹田 栄作
東京都千代田区丸の内二丁目2番3号 三
菱電機株式会社内

(72)発明者 小川 雅春
東京都千代田区丸の内二丁目2番3号 三
菱電機株式会社内